Picard Group $\xrightarrow{understand}$ Diophantine equations?

Sachin Kumar
University of Waterloo, Faculty of Mathematics

Abstract

Why should a number theorist be interested in algebraic geometry? In this essay we hope to demonstrate one very good reason, by showing essentially geometric reasons why certain Diophantine equations fail to have solutions. But we will begin by placing the study of Diophantine equations into the context of algebraic geometry, to see how techniques from many different realms of mathematics can be useful in their study.

1 Why algebraic geometry for a number theorist?

Suppose that we are interested in studying the integer or rational solutions to a polynomial equation $f \in \mathbb{Z}[X_0, X_1, \ldots, X_n]$. We assume f to be homogeneous, so that the sets of rational and integer solutions concide: more precisely, any integer solution may be turned into a rational one by clearing denominators. We wish to define a geometric object X as

$$X = \{f = 0\} \subset \mathbb{P}^n \tag{1}$$

so that X is the zero-set of the polynomial f in projective space. This is, as it stands, not a definition at all. What we really mean is, for example,

$$X(\mathbb{Q}) = \{[X_0 : \cdots : \ldots, X_n] \in \mathbb{P}^n(\mathbb{Q}) \mid f(X_0, \ldots, X_n) = 0\} \tag{2}$$

where $\mathbb{P}^n(\mathbb{Q})$ is the set of $(n+1)$-tuples of rational numbers, modulo multiplying them all through by a common factor. Given that f has integer coefficients, we can take any $(n+1)$-tuple of elements of any ring R and substitute it into f, and so define $X(R)$ in exactly the same way, replacing $\mathbb{Q}$ by R in the definition (2) above. In this way we can consider the sets $X(\mathbb{R})$, $X(\mathbb{C})$, $X(\mathbb{F}_p)$ and so on. There are obvious maps between some of these sets: for example, $\mathbb{Q}$ is contained in $\mathbb{R}$ and so $X(\mathbb{Q})$ is contained in $X(\mathbb{R})$.

Remark 1.1 What we have defined here is a mapping $R \mapsto X(R)$ which is actually a functor from the category of commutative rings to that of sets. This functor is the *functor of points* of the scheme X defined in (1). This way of looking at schemes can be very profitable: see [2, Chapter VI] for an explanation.

In Figure 1, several of these point sets are shown. The one which really interests us is $X(\mathbb{Q})$, the set of rational solutions to our polynomial equation. Unfortunately, this is also the point set we know least about. The object of studying the algebraic geometry of X is to use techniques available over the various fields other than $\mathbb{Q}$ to deduce facts about $X(\mathbb{Q})$. For example:

- On $X(\mathbb{R})$, we can use real analysis. For example, if X is smooth then $X(\mathbb{R})$ is a real manifold. In particular, it is easy to check whether $X(\mathbb{R}) = \emptyset$, and if $X(\mathbb{R}) = \emptyset$, then $X(\mathbb{Q})$ is certainly empty too!

- On $X(\mathbb{C})$, we have all the tools available to study complex analytic varieties. For example, $X(\mathbb{C})$ has cohomology groups which give much information about its geometry, and these come with Hodge decompositions.
- It may not be obvious that much can be said about $X(\bar{\mathbb{Q}})$ However, a general idea known as the *Lefschetz principle* says that any algebraic fact which can be proved about $X(\mathbb{C})$, whether or not the proof uses methods outside algebra, also applies to $X(\bar{\mathbb{Q}})$ and indeed to $X(K)$ where K is any algebraically closed field of characteristic zero. In particular, in this paper we will use the fact that the Picard groups of X over $\bar{\mathbb{Q}}$ and over $\mathbb{C}$ are the same, and will often identify them.
- Given that X is defined over $\mathbb{Q}$, many objects associated to X over $\bar{\mathbb{Q}}$ come equipped with an action of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. In particular, the point set $X(\mathbb{Q})$ and the Picard group Pic $(X_{\bar{\mathbb{Q}}})$ have Galois actions, and we can use Galois theory to deduce results about the corresponding objects over $\mathbb{Q}$.
- In the same way that $X(\mathbb{Q})$ embeds into $X(\mathbb{R})$, it also embeds into $X(\mathbb{Q}_p)$ for any prime p. Again, $X(\mathbb{Q}_p)$ can be studied by analytic methods, and in particular it is straightforward to decide whether $X(\mathbb{Q}_p)$ is empty for any given p.
- Given that X is a projective variety, any point in $X(\mathbb{Q}_p)$ can be represented as $[x_0 : \cdots : x_n]$ where the x_i all lie in $\mathbb{Z}_p$ and are not all divisible by p. This point then has a well-defined reduction modulo p, and so we get a map from $X(\mathbb{Q}_p) \to X(\mathbb{F}_p)$. Often, the study of $X(\mathbb{Q}_p)$ actually comes down to the study of $X(\mathbb{F}_p)$, especially when p is a prime of good reduction for X. Varieties over finite fields have many advantages - in particular, they have only finitely many points which can therefore be listed!
- Finally, a rather more deep and complicated link exists between the geometry of $X(\bar{\mathbb{F}}_p)$ and that of $X(\mathbb{C})$, given by the Weil conjectures. We will not discuss this link at all in this course, but mention it as a powerful example of the application of algebraic geometry to arithmetic.

2 The Picard group

Given a set of polynomial equations defined over $\mathbb{Q}$, we aim to study their rational solutions by considering the geometry of the variety X which they define. One geometric invariant which has a great effect on the arithmetic is the Picard group of X, and we will devote some time to the general definition of the Picard group and to understanding its structure for some specific surfaces.

2.1 Definition of the Picard group

One way to see the construction of the Picard group is to try to mimic the construction of the homology groups of a manifold. In that case, we form a free group of “cycles” and take the quotient by a subgroup of “boundaries”. In the case of algebraic varieties, it is reasonable to replace the cycles by algebraic subvarieties. However, there is nothing immediately obvious to replace the boundaries, since a subvariety does not have a boundary. Many ways have been devised to solve this problem in arbitrary codimension, but in codimension one there is one which is particularly straightforward to define.

In what follows, X will be a *smooth* irreducible variety over a field k.

Definition 2.1. A *prime divisor* on a smooth variety X over a field k is an irreducible closed subvariety $Z \subset X$ of codimension one, also defined over k. A *divisor* is a finite formal linear combination $D = \sum_i n_i Z_i$ with $n_i \in \mathbb{Z}$ of prime divisors. The group of divisors on X, which is the free group on the prime divisors, is denoted Div X.

Remark 2.2. A prime divisor is not required to be nonsingular.

Remark 2.3. If X is a variety over a field k which is not algebraically closed, then a prime divisor may not be geometrically irreducible. For example, the 0-dimensional variety $\{x^2 = 2\} \subset \mathbb{A}^1_{\mathbb{Q}}$ is irreducible as a variety over $\mathbb{Q}$ and is therefore a prime divisor on $\mathbb{A}^1_{\mathbb{Q}}$.

Definition 2.4. A divisor $D = \sum_i n_i Z_i$ is effective if $n_i \geq 0$ for all i.

Definition 2.5. The *support* of a divisor D, written supp D, is the closed subset of X given by

$$\operatorname{supp}\left(\sum_i n_i Z_i\right) = \bigcup_{n_i \neq 0} Z_i$$

To define an equivalence relation on divisors, we use the rational functions on X. For any prime divisor Z on X, we would like to define the valuation of a function f along that divisor. Since X is smooth, the local ring $\mathcal{O}_{X,Z}$ is a discrete valuation ring and so defines a discrete valuation v_Z on its field of fractions. This is simply the function field $\kappa(X)$ of X, so we get a discrete valuation $v_Z : \kappa(X) \to \mathbb{Z}$ for each prime divisor D.

If $v_Z(f) = d > 0$, then we say that f has a *zero of order* d along Z (and, indeed this happens if and only if f vanishes at almost all points of Z). If $v_Z(f) = -d < 0$, then we say that f has a *pole of order* d along Z. If $v_Z(f) \geq 0$ then f is *regular* at Z.

Using the valuations, we can associate a divisor to any rational function f.

Definition 2.6. Let $f \in \kappa(X)$ be a rational function on X. We define the *divisor* of f to be

$$\operatorname{div} f = (f) = \sum_Z v_Z(f) Z$$

where the sum is taken over all prime divisors $Z \subset X$.

Remark 2.7. This sum is finite - that is, $v_Z(f) = 0$ for all but finitely many prime divisors Z. To see this, write f as a quotient of two polynomials; they are each zero only on a closed subset of codimension one in X, which is therefore the union of finitely many prime divisors.

Definition 2.8. A divisor which is of the form (f) for some $f \in \kappa(X)$ is called a *principal divisor.* The subgroup of Div X consisting of the principal divisors is denoted by Princ X.

Definition 2.9. Two divisors $D, D' \in$ Div X are *linearly equivalent*, written $D \sim D'$, if their difference $D - D'$ is principal.

Example 2.10. Suppose that D and D' are two effective divisors, with disjoint supports, which are linearly equivalent. Then, by definition, there is a function $f \in \kappa(X)$ such that $(f) = D - D'$. Now the function f defines a rational map from $X \to \mathbb{P}^1_k$, such that $f^{-1}(0) = D$ and $f^{-1}(\infty) = D'$. The other fibres of this rational map are all effective divisors which are also linearly equivalent to D, so give a "family" of effective divisors "moving" from D to D'.

We can now define the Picard group of a smooth variety.

Definition 2.11. Let X be a smooth variety. The *Picard group* of X is the quotient group

$$\text{Pic } X = \text{Div } X/\text{Princ } X$$

Remark 2.12. For a general (not necessarily smooth) variety X, what we have defined is not the Picard group, but the *Weil divisor class group.* The Picard group in general is the group of isomorphism classes of line bundles on X. If X is normal, we can define a *Cartier divisor* to be a divisor Z which is locally principal: that is, each point of supp Z has a neighbourhood is which Z is principal. For an irreducible normal variety, the Picard group is isomorphic to the group of Cartier divisors modulo linear equivalence. This is equal to the Weil divisor class group if X is locally factorial and, in particular, if X is smooth. For a thorough treatment of these ideas, see Section II.6 of [3].

Example 2.13. Pic $\mathbb{A}^n = 0$ for any $n \geq 1$. To prove this, we must show that any irreducible subvariety of codimension one in $\mathbb{A}^n$ may be defined by a single polynomial. This reduces to the algebraic fact that, in a unique factorisation domain, any prime ideal of height one is principal. For a proof, see [1, Corollary 10.6].

Example 2.14. Let D be a divisor on a smooth variety X and let P be a point of X. Then D is linearly equivalent to a divisor D' with $P \notin \text{supp } D'$. For the local ring $\mathcal{O}_{X,P}$ is a unique factorisation domain, and so by using the same result as the previous example we can find a neighbourhood U of P and a function f such that, after restricting to U, $(f) = D$. Therefore $D' = D - (f)$ is a divisor linearly equivalent to D and with support avoiding P.

Example 2.15. Given a surface $X \subset \mathbb{P}^3$, a *plane section* is the divisor on X defined by intersecting X with a plane (and, if necessary, counting the components with the correct multiplicities). Any two plane sections of X are linearly equivalent. For let D_1 and D_2 be the intersections of X with distinct planes defined by linear forms l_1 and l_2 respectively. Then the quotient l_1/l_2 defines a rational function on X, with divisor $(l_1/l_2) = D_1 - D_2$.

More generally, let $X \subseteq \mathbb{P}^n$ be any projective variety. For the same reason, any two hyperplane sections of X are linearly equivalent. We will often talk of "the" hyperplane section to mean the class in Pic X of a hyperplane section.

Remark 2.16. Bertini's Theorem [3, Chapter II, Theorem 8.8] shows that, if X is smooth and k algebraically closed, then almost all hyperplane sections of X are nonsingular. Generalisations of this result can give many consequences of the form "Any divisor D is equivalent to a difference $A - B$ with A, B effective and nice", where nice can mean, for example: smooth; avoiding a given finite set of points; transverse to a given finite set of subvarieties; and so on.

Claim 1. Let Z be a prime divisor in a smooth variety X, and let U denote the complement $X \setminus Z$. Then the following sequence holds:

$$\mathbb{Z} \to Pic\ X \to Pic\ U \to 0$$

where the first map is $1 \mapsto Z$ and the second $D \mapsto D \cap U$, is exact. Using the sequence, we can show that Pic $\mathbb{P}^n \cong \mathbb{Z}$ for any $n \geq 1$.

2.2 Different ground fields

If the ground field k of the variety X is not algebraically closed, then the above definitions are still valid. We have

$$\text{Pic } X = \frac{\text{Div } X}{\text{Princ } X} = \frac{\text{Divisors defined over } k}{\text{Divisors of functions defined over } k}$$

On the other hand, we can also consider the base extension $\bar{X}$ of X to $\bar{k}$, and its Picard group. This is

$$\text{Pic } \bar{X} = \frac{\text{Div } \bar{X}}{\text{Princ } \bar{X}} = \frac{\text{Divisors defined over } \bar{k}}{\text{Divisors of functions defined over } \bar{k}}$$

There is a natural homomorphism $i : \text{Pic } X \to \text{Pic } \bar{X}$, given by the inclusion $\text{Div } X \subseteq \text{Div } \bar{X}$. The Galois group $\text{Gal}(\bar{k}/k)$ acts on $\text{Pic } \bar{X}$, and the image of i lies in the Galois-fixed subgroup $(\text{Pic } \bar{X})^{\text{Gal}(\bar{k}/k)}$. We state a few facts about the map i.

- $\text{Div } X = (\text{Div } \bar{X})^{\text{Gal}(\bar{k}/k)}$ that is, a divisor is defined over k if and only if it is fixed by the Galois action. This is a restatement of Remark ??.
- If X is a projective variety, then i is injective. This comes down to saying that if a divisor D is defined over k and is the divisor of a function defined over $\bar{k}$, then it is in fact the divisor of a function defined over k. This is an easy consequence of Hilbert's Theorem 90 (Proposition ??).
- If k is a number field and X has points everywhere locally - that is, $X(k_v) \neq \emptyset$ for all places v of k - then i is an isomorphism. This is a consequence of the Hasse principle for Severi-Brauer varieties.

2.3 Intersection numbers

In this section, we let X be a smooth surface over a field k. Given two curves in X, they will generally intersect in a finite number of points. The number of points is called their intersection number, and it gives us a very useful bilinear form on the Picard group.

We say that two curves C_1, C_2 on X *intersect transversely* at a point $P \in C_1 \cap C_2$ if, in the local ring $\mathcal{O}_{X,P}$, there are functions f_1, f_2 which generate the unique maximal ideal and are such that $(f_i) = C_i$ on a neighbourhood of P. This definition corresponds to the intuitive notion that the curves are nonsingular at P and have distinct tangent directions.

Definition 2.17. Let X be a smooth surface over a field k, and let D and D' be two prime divisors on X which intersect transversely. We define the intersection number of D and D' to be $D \cdot D' = |D \cap D'|$ where the cardinality of the intersection $D \cap D'$ is taken over the algebraic closure of k.

Theorem 2.18. *Let X be a smooth surface. The intersection number extends to a symmetric bilinear pairing* $\text{Div } X \times \text{Div } X \to \mathbb{Z}$ *which respects linear equivalence, and hence to a symmetric bilinear pairing* $\text{Pic } X \times \text{Pic } X \to \mathbb{Z}$.

Proof. See [3, Chapter V, Theorem 1.1]. ॐ

Definition 2.19. Let X be a smooth surface and D a divisor in X. The *self-intersection number* of D is the intersection number $D^2 = D \cdot D$.

Example 2.20. Any two distinct lines in $\mathbb{P}^2$ intersect in precisely one point, so have intersection number 1. Moreover, any line is linearly equivalent to any other line. We deduce that the self-intersection number of a line in $\mathbb{P}^2$ is 1.

Example 2.21. Let $X \subseteq \mathbb{P}^n$ be a projective surface, and let H be a hyperplane section of X. Then H^2 is the *degree* of X, defined to be the number of points of intersection of X with any sufficiently general linear subspace of dimension $n-2$. To see this, use the fact that $H^2 = H_1 \cdot H_2$ where H_1 and H_2 are any two sufficiently general hyperplane sections of X.

Claim 2. Suppose that X is a smooth hypersurface in $\mathbb{P}^3$ defined by a single equation of degree d, then $\deg X = d$.

Example 2.22. Let $X \subseteq \mathbb{P}^n$ be a projective surface, and let C be an irreducible curve on X. Then $H \cdot C$ is the *degree* of C, defined to be the number of points of intersection of C with a sufficiently general hyperplane.

Claim 3. Let X be the projective quadric surface $xy = zw$, and let U be the open subset defined by $w \neq 0$. Then $U \cong \mathbb{A}^2$ and deduce that Pic $U = 0$. $X \setminus U$ consists of two straight lines. Using the exact sequence (from *Claim 1.*), we have Pic $X \cong \mathbb{Z}^2$, generated by the classes of these two straight lines.

Proof idea. To proof that the two lines are not equivalent, we may use intersection numbers. ॐ

The intersection number defines a new equivalence relation on divisors on a surface.

Definition 2.23. Let X be a smooth surface. Two divisors D and D' on X are said to be *numerically equivalent* if $D \cdot E = D' \cdot E$ for all divisors E on X.

Given that intersection numbers respect linear equivalence, this gives an equivalence relation coarser than linear equivalence. The subgroup of classes in Pic X which are numerically equivalent to 0 is denoted by Pic $^n X$.

2.4 Structure of Picard Group over $\mathbb{C}$

When X is a smooth projective variety over the complex numbers $\mathbb{C}$, one can use methods from the theory of analytic varieties to deduce results about the Picard group of X. Here we mention briefly some useful facts arising from this.

There is an exact sequence of analytic sheaves on X known as the *exponential sequence*, which gives rise to an exact sequence of cohomology groups:

$$H^1(X(\mathbb{C}), \mathbb{Z}) \to H^1(X, \mathcal{O}_X) \to \text{Pic } X \to H^2(X(\mathbb{C}), \mathbb{Z})$$

We state several interesting facts about this sequence.

- Since X is a smooth projective variety, $X(\mathbb{C})$ is a compact manifold. Its integral cohomology groups $H^i(X(\mathbb{C}), \mathbb{Z})$ are therefore finitely generated abelian groups.
- The group $H^1(X, \mathcal{O}_X)$ is a finite-dimensional complex vector space, and it turns out that $H^1(X(\mathbb{C}), \mathbb{Z})$ is a lattice in this vector space. The image of $H^1(X, \mathcal{O}_X)$ in Pic X is therefore

a complex torus, and in fact is an Abelian variety. It is denoted $\mathrm{Pic}^0 X$, and lies inside the kernel $\mathrm{Pic}^n X$ of the intersection pairing.

- The image of Pic X in $H^2(X(\mathbb{C}), \mathbb{Z})$ is isomorphic to Pic $X/\mathrm{Pic}^0 X$, and this is therefore a finitely generated abelian group, called the Néron-Severi group of X.

For more background to these results, see Appendix B of [3].

References

[1] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1995.

[2] D. Eisenbud and J. Harris. *The geometry of schemes*, volume 197 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2000.

[3] R. Hartshorne. *Algebraic geometry*, volume 52 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1977.

[4] Martin Bright. *The Picard group*, 2008